NPSI SPECIAL BRIEFING №01

NOTHING LEFT TO REDACT

Zero secrets

Canada's data already answers to American law. The new generation of military AI turns that exposure into a complete intelligence picture. A wake-up call for the people who still think residency is sovereignty.

Author	Imprint	Date	Classification
Jesse James	NPSI · npsi.ca	June 11, 2026	Unclassified — all sources open

EXECUTIVE SUMMARY

The bottom line

Read this page and you have 80% of the briefing

Canada effectively holds no data secrets from the United States. Not because we are careless, and not because we chose transparency — because of architecture. The overwhelming majority of Canadian government, corporate, and citizen data sits on infrastructure owned by three American corporations, and under the US CLOUD Act and FISA Section 702, American jurisdiction follows corporate ownership, not server location. A US warrant for data in Toronto is as enforceable as one for Redmond.

This stopped being a legal theory on June 10, 2025, when Microsoft France's director of public and legal affairs, Anton Carniaux, was asked under oath by the French Senate whether he could guarantee that French citizens' data would never reach US authorities. His answer: *"No, I cannot guarantee that."* The same answer applies to Canada. Microsoft's December 2025 pledge of C$19 billion in Canadian AI infrastructure — complete with a five-point "digital sovereignty" plan — does not change the law it operates under. The company admitted as much in Paris.

The stakes have changed because the technology has. AI-driven sensor and data fusion now converts raw data exhaust into real-time targeting pictures: the Pentagon's Maven Smart System prosecuted roughly 1,000 targets in the first 24 hours of the 2026 Iran operation and 13,000 targets in 38 days. The capability class is what matters for Canada: whoever controls the infrastructure layer a nation's data transits can, in principle, denoise that nation into permanent legibility. Allies have done this to allies before — the NSA tapped Angela Merkel's communications through Danish cables — and foreign-controlled infrastructure has already been used as policy leverage against a partner at war, when Starlink declined coverage over Crimea.

The Carney government's sovereign AI agenda — the $2-billion Sovereign AI Compute Strategy, the June 2026 "AI for All" strategy — is real and material. But its flagship Cohere data centre is operated by a New Jersey company, and the federal definition of "sovereign" still leans on geography instead of jurisdiction. This briefing recommends a three-stage response: adopt a control-based definition of sovereign infrastructure, move classified and defence workloads to genuinely Canadian-controlled systems, and use the Investment Canada Act and the new $500-million Canadian Tech Growth Fund to ensure Canada's AI champions are not acquired before scale — the pattern that took Nortel's patents and Element AI.

KEY FINDINGS

Six findings, each one a structural fact

4×	13,000	$0.12	C$19B
Federal Azure consumption vs. AWS since FY2019–20 — Microsoft is the Government of Canada's dominant cloud. [SSC evaluation, 2024–25]	Targets prosecuted in 38 days through Maven Smart System during Operation Epic Fury, per the Pentagon's Chief Digital & AI Officer. [Breaking Defense, May 2026]	Price per record at which Duke researchers legally purchased US military-personnel data from commercial brokers. [Duke Sanford School, 2023]	Microsoft's 2023–2027 Canadian commitment — deepening the dependence its own Senate testimony concedes it cannot shield. [Microsoft, Dec 2025]

01 **Most Canadian cloud usage runs on foreign infrastructure — and the famous statistic needs honest attribution.**

The widely repeated claim that "over 80 percent of Canadian cloud services rely on foreign infrastructure" traces to IDC Canada's *Canadian Cloud Services Market Analysis* (2024) — private market research, not a Government of Canada figure, though it has been mis-cited as one. Ottawa's own position is qualitative and damning enough: "As long as a CSP that operates in Canada is subject to the laws of a foreign country, Canada will not have full sovereignty over its data." [TBS White Paper on Data Sovereignty and Public Cloud, 2018–2023; IDC Canada 2024, via Balsillie Papers]

02 **Jurisdiction follows ownership, not geography.**

The US CLOUD Act (18 U.S.C. §2713, enacted March 2018) compels any US-controlled provider to produce data in its "possession, custody or control" regardless of storage location. FISA Section 702 reaches the same providers for foreign-intelligence collection. No Canada–US CLOUD Act bilateral agreement exists as of early 2026, so the exposure is one-directional: Washington reaches Canadian data directly; Ottawa still queues through MLAT. [18 U.S.C. §2713; Balsillie Papers, 2026]

03 **Microsoft confirmed the exposure under oath.**

Carniaux's June 10, 2025 French Senate testimony converted a decade of legal debate into an on-the-record corporate admission. Canadian analysts noted immediately that the identical logic covers Canadian data on Azure, AWS, Google Cloud — and Starlink. [French Senate hearing transcript, June 10, 2025; Canadian Cyber in Context]

04 **The acquisition risk is real but the sharper exposure is the operating layer.**

Canada's largest data-centre operator, eStruxture, was recapitalized in a CA$1.8-billion deal led by Toronto's Fengate Asset Management (closed October 2024) — Canadian control retained, US private-markets investors participating. The harder problem: Cohere's $725-million flagship facility, backed by up to $240 million in federal funding, is operated in Cambridge, Ontario by New Jersey-based CoreWeave. [Fengate/eStruxture announcements, 2024; ISED AI Compute Challenge award]

05 **The Carney agenda is substantial — and partly built on the thing it is trying to escape.**

The $2-billion Sovereign AI Compute Strategy (December 2024) and the ~$2.3-billion "AI for All" strategy (June 4, 2026) are genuine commitments, targeting 850 MW of compute by 2030 and a $500-million Canadian Tech Growth Fund. Five days after Microsoft's C$19-billion Canadian pledge, experts pointed out the contradiction: sovereignty isn't determined by where the data centres sit, but by which company runs the servers. [ISED; PMO, June 4, 2026; Microsoft, Dec 9, 2025; Blayne Haggart, Brock University]

06 **The threat is demonstrated, not hypothetical.**

Maven Smart System fused satellite, drone, SIGINT, and geolocation feeds into a single targeting picture at operational tempo in 2026. Allies have structurally surveilled allies (Operation Dunhammer). US data brokers sold military-personnel records for as little as $0.12 each. Starlink coverage was withheld from a partner's operation as a matter of one company's policy. Every mechanism in this briefing has already been used. [Breaking Defense, May 2026; Danish DR / Operation Dunhammer, 2021; Duke Sanford School, Nov 2023]

SECTION 01

Residency is not sovereignty

All three hyperscalers operate Canadian regions. All three are American corporations. Those two sentences do not cancel each other out — the second one wins.

Azure runs regions in Toronto and Québec City; AWS and Google Cloud in Montréal and Toronto. The marketing term for this is "data residency," and it answers exactly one question: where the bytes physically sit. Sovereignty answers a different question: whose law governs access to them. A Canadian data centre operated by a US company is a US-jurisdictioned service with a Canadian postal code.

The mechanics are unambiguous. The CLOUD Act applies to any provider with sufficient US "minimum contacts," not only US-headquartered firms. Selecting a Canadian region changes residency, not jurisdiction. Customer-managed encryption keys mitigate but do not eliminate the exposure: metadata, account information, file names, sharing structures, and activity logs remain compellable, and data must be decrypted in memory during active processing — a residual access window no contract clause closes. FISA 702 was reauthorized in 2024 and runs through April 2026, with the reauthorization fight ongoing in Washington as this briefing publishes. [18 U.S.C. §2713; FISA Reform and Reauthorization Act, 2024]

The federal footprint

Shared Services Canada is the central IT provider for 43 federal organizations, historically operating roughly 700 data centres running some 14,000 applications. Per SSC's own 2024–25 evaluation, Azure is the most-used cloud in the federal government, with cumulative consumption since FY2019–20 running four times that of AWS. The Privacy Commissioner's 2023–24 annual report states the principle plainly: "data residency requirements alone cannot guarantee protection from foreign legal processes." [SSC Cloud Services Evaluation, 2024–25; OPC Annual Report, 2023–24]

The defence exposure

DND/CAF run common collaboration on "Defence 365," a defence-tailored Microsoft 365 deployment spanning the Defence Team and partner departments. Analysis published in the Balsillie Papers argues data on these systems could, in theory, be compelled by US authorities without Canadian judicial review. That is an analytical claim, not a documented disclosure event — this briefing labels it as such — but the architecture that makes it possible is not in dispute. [Balsillie Papers, Appleton, March 11, 2026 — analytical assessment]

Canada's own defence AI posture compounds the gap. The 2024 DND/CAF AI Strategy commits the Defence Team to being "AI enabled by 2030" and invokes "sovereign AI foundations" — but uses "sovereign" to mean indigenous capability, not data jurisdiction. The Communications Security Establishment's AI strategy is blunter about urgency ("we simply cannot afford to wait or we will be left

behind") and reported hostile actors used AI against 27% of elections worldwide in 2023–2024. [DND/CAF AI Strategy, March 2024; CSE AI Strategy; CSE Democratic Process Update, 2025]

SECTION 02

The acquisition layer: who buys the pipes, who runs the racks

The marquee Canadian data-centre deal stayed Canadian. The flagship sovereign AI facility did not stay Canadian-operated. Both facts should inform policy.

eStruxture — fifteen facilities across Montréal, Toronto, Calgary, and Vancouver, the country's largest operator — was recapitalized for CA$1.8 billion in 2024, the largest transaction in Canadian data-centre history. Toronto's Fengate Asset Management led; CDPQ exited; US private-markets investors Partners Group and Pantheon took secondary positions; majority control stayed with Fengate and the Wener Family Office. This is the template: foreign capital welcomed, Canadian control retained. [Fengate/eStruxture, June–October 2024]

The CoreWeave arrangement is the counter-template. The first award under the $700-million AI Compute Challenge — up to $240 million in federal funding anchoring Cohere's $725-million project — flows through a facility in Cambridge, Ontario operated by New Jersey-based CoreWeave. Denvr Dataworks' CEO called federal funds flowing to a US operator "ridiculous." Minister Evan Solomon's defence — "What I don't want to do is a purity test on sovereignty" — is honest about the trade-off, and it concedes the point: the operating layer of Canada's flagship sovereign compute is American. Telus's sold-out Sovereign AI Factory in Rimouski runs on NVIDIA hardware; Bell's AI Fabric leases capacity to Groq, Cerebras, and CoreWeave. Sovereign-branded, foreign-supplied. [ISED; The Logic; corporate announcements, 2025]

The Investment Canada Act is sharpening — use it

Bill C-34 took effect through 2024. On March 5, 2025 — amid the tariff confrontation — updated National Security Review Guidelines introduced an "economic security" factor, incorporated the new Sensitive Technology List (which names artificial intelligence, quantum, and advanced digital infrastructure among eleven sensitive areas), and made sensitive personal data — health, genetic, biometric, geolocation, and data on government, military, and intelligence officials — an explicit national-security consideration. There were 1,138 ICA filings in FY2024–25, the third-highest on record. Counsel at DLA Piper now advise that AI and digital-infrastructure investments face "a presumption of risk." The legal architecture for defending the asset class exists. What remains is the will to apply it before a sale, not after. [ISED National Security Review Guidelines, March 5, 2025; Sensitive Technology List, Feb 6, 2025; DLA Piper]

SECTION 03

Ottawa's answer, audited

The Carney government is spending real money on the right problem. The audit question is whether the definition of "sovereign" underneath the spending can survive contact with the CLOUD Act.

The Canadian Sovereign AI Compute Strategy ($2 billion, Budget 2024, launched December 2024) has three pillars: up to $700 million mobilizing private investment through the AI Compute Challenge; up to $1 billion in public supercomputing, including up to $705 million for the AI Sovereign Compute Infrastructure Program and a secure SSC/NRC facility for national-security research; and the $300-million AI Compute Access Fund, open since March 2025. Partnerships now being finalized are stated to deliver 850 MW of compute by 2030, scalable to 2.3 GW. [ISED, Canadian Sovereign AI Compute Strategy]

"AI for All," announced by the Prime Minister on June 4, 2026, layers on roughly $2.3 billion more: up to 90,000 AI jobs for young Canadians, a target of 250,000 new jobs through AI adoption by 2031, raising business AI adoption from 12% to 60% by 2034, a $700-million top-up to the Compute Access Fund, $130 million for commercialization across Vector, Mila, and Amii, a $500-million Canadian Tech Growth Fund taking federal equity stakes in promising AI firms — and twelve international AI partnerships signed since March 2025, from Germany to the UAE. The strategy pledges to "build the foundations of sovereign Canadian AI." NDP critic Don Davies called it rushed and warned it leaves "Canadians dangerously exposed." [PMO, June 4, 2026; The Register, June 4, 2026]

The Microsoft contradiction

On December 9, 2025, Microsoft committed C$7.5 billion over two years within a C$19-billion 2023–2027 Canadian program — "the most important commitment in Microsoft Canada's history," per Brad Smith — expanding Azure Canada Central and Canada East, attaching a five-point digital-sovereignty plan ("keep Canadian data on Canadian soil," an Ottawa Threat Intelligence Hub, customer-controlled keys), and pledging litigation against any order to suspend Canadian operations. [Microsoft On the Issues, Dec 9, 2025]

> *"Sovereignty isn't determined by where your data centres are located, but by which company runs the servers... Microsoft admitted in a June hearing before the French Senate that they have to follow U.S. law under the Cloud Act."*
>
> — Blayne Haggart, Brock University, December 16, 2025

Hold both facts at once. Microsoft's investment deepens the dependence, and Microsoft's own sworn testimony concedes the dependence cannot be contractually shielded. The corporate sovereignty pledge and the corporate legal admission cannot both be operative. The law wins.

SECTION 04

The machine that reads everything

For thirty years, the comfort was that nobody could process it all. That comfort is gone. The denoising problem has been solved at operational tempo, and the proof is public.

Palantir's Maven Smart System — successor to Project Maven, with Palantir as primary partner after Google's 2018 withdrawal — consolidated nine separate Department of Defense targeting tools into one interface fusing satellite imagery, drone footage, signals intelligence, and geolocation feeds. During Operation Epic Fury, which began February 28, 2026, the Pentagon's Chief Digital and AI Officer told the SCSP AI+Expo that the system was used "to conduct strike missions across the entire battle space — 13,000 targets in 38 days." The Washington Post reported roughly 1,000 targets struck in the first 24 hours. The Pentagon awarded Palantir a $480-million expansion in 2024 and has sought roughly $2.3 billion in further Maven funding. [Breaking Defense, May 12, 2026; Washington Post; CSIS; C4ISRNET]

This briefing makes no operational claims and proposes no surveillance systems. The point is capability-class: the technology that converts massive multi-modal data flows into a coherent real-time picture is mature, commercial, and scaling. A nation whose government communications, energy-grid telemetry, health records, financial flows, and network metadata all transit foreign-controlled infrastructure is **permanently legible** to the power that controls that infrastructure. Friend or not.

Allies do this to allies

Operation Dunhammer — a Danish Defence Intelligence Service internal investigation conducted 2014–15 and revealed in May 2021 — confirmed the NSA used Danish underwater-cable access and the XKeyscore system to surveil Chancellor Angela Merkel, Frank-Walter Steinmeier, Peer Steinbrück, and other senior European officials from 2012 to 2014. Denmark: a small, loyal, "super-Atlanticist" NATO ally, dependent on US security guarantees, hosting US access against its closest neighbours. The structural parallel to Canada requires no elaboration. [Danmarks Radio / Operation Dunhammer disclosures, May 2021]

You don't even need an agency — there's a market

The US commercial data-broker ecosystem is estimated at roughly $200 billion across more than 750 registered brokers. Duke University researchers legally purchased US military-personnel records — names, addresses, health and financial attributes — through a .org and a .asia domain for as little as $0.12 per record, $0.01 in bulk, covering up to roughly 45,000 service members. In March 2026, the FBI Director declined before the Senate to commit to not purchasing Americans' location data. Canadian-relevant data flows through the same brokers, purchasable by allies and adversaries alike, no warrant required. [Duke Sanford School of Public Policy, Sherman et al., Nov 6, 2023; Senate testimony, March 2026]

Starlink: the canonical lesson

In 2022, coverage over Russian-occupied Crimea was withheld during a Ukrainian naval-drone operation — one company's decision constraining one nation's war. Ukraine's dependence on at least 47,000 terminals is simultaneously lifeline and vulnerability. Foreign Policy stated the principle exactly: when a private supplier can decide which operations a front-line state is permitted to conduct, the relationship has ceased to be commercial — it is a delegation of sovereignty. Prime Minister Carney invoked the Crimea episode directly in March 2026 while championing Telesat Lightspeed as Canada's $7-billion sovereign alternative. The lesson has been absorbed for satellites. It has not yet been absorbed for clouds. [Foreign Policy; PMO remarks, March 9, 2026]

One more data point on the reliability of goodwill: the Biden administration's AI Diffusion Rule (January 15, 2025) sorted the world into three tiers of access to American chips and model weights — placing NATO allies in the second tier — and the Trump administration rescinded it on May 13, 2025, two days before it took effect. US technology policy toward allies now reverses on a change of administration. Planning national infrastructure on its continuity is not strategy; it is hope. [US Department of Commerce, BIS, 2025]

SECTION 05

What sovereign actually looks like

Four models exist. France regulates ownership. Europe builds standards. The Gulf buys managed interdependence. Canada has better raw inputs than any of them — and the worst record of keeping what it builds.

MODEL	MECHANISM	WHAT CANADA SHOULD TAKE
France — SecNumCloud 3.2	ANSSI standard: EU-only control (non-EU shareholders capped <25% individually, 39% collectively, no veto), immunity from extraterritorial law required. Sensitive state data must run on qualified clouds. Mistral deployed on Outscale. €109B AI-infrastructure push (Feb 2025).	The control-based definition of "sovereign." Caveat: ITIF and US critics call the ownership caps protectionist and a potential WTO problem — study before importing wholesale.
EU — Gaia-X / EuroStack	Standards-led; November 2025 Declaration for European Digital Sovereignty. European Parliament estimates >80% reliance on non-EU digital products — a mirror of Canada's position.	Procurement preference as industrial policy; coalition leverage with non-US partners.
Gulf — G42 / HUMAIN	Managed interdependence: local governance and residency paired with access to global model catalogs (G42–Microsoft).	Honesty that full autarky isn't the goal — control of the sensitive tier is.
Japan / India — GENIAC / IndiaAI	State-funded national compute missions (IndiaAI ≈ US$1.2B / ₹10,372 crore).	Sustained public compute funding as baseline, not one-time announcement.

Canada's hand is strong

Abundant low-carbon hydro in Quebec, BC, and Manitoba; a cold climate that lets facilities like Telus's Rimouski plant run on natural air cooling at roughly three times industry energy efficiency; Cohere, valued at US$5.5–6.8 billion, as a genuine sovereign foundation-model champion; the Hinton–Bengio research legacy institutionalized in Vector, Mila, and Amii; Telesat Lightspeed — Canadian-owned LEO connectivity backed by a $2.14-billion federal loan, $400 million from Quebec, and a >$5-billion Telesat/MDA military satcom contract signed December 2024, now designated a sovereign capability in the defence industrial strategy; and the CANARIE national research network. Few countries hold all five cards: energy, climate, talent, a champion firm, and sovereign connectivity. [Corporate and government announcements, 2024–2026]

And Canada's record is the warning

Nortel: roughly $400 billion in market value at peak, about 35% of the TSX, carrying an estimated three-quarters of North America's internet backbone — bankrupt by 2009, patents dispersed abroad. Element AI: Canada's flagship AI startup, Bengio-backed, roughly US$250 million raised — sold to California's ServiceNow in 2020 for about US$230 million, acquired for its patents and people, founders' equity largely wiped out, Ottawa's pending $20-million contribution cancelled. Jim Balsillie called it "a cautionary tale for governments falling prey to hype." The pattern is consistent: Canada builds, Canada underdefends, Canada sells before scale. Cohere is the live test of whether the pattern holds. [Public record; Balsillie, 2020]

RECOMMENDATIONS

Three stages, seven moves

STAGE 1 · 0–6 MONTHS

Define and triage

1. Adopt a **control-based definition of sovereign cloud** — jurisdictional control (no foreign-compellable parent), operational control (Canadian-accountable administration), cryptographic control (Canadian-held keys), and audit control. All four, or it isn't sovereign.

   BENCHMARK → Any documented CLOUD Act or FISA 702 request touching GC data triggers immediate escalation.

2. Mandate **Transfer Impact Assessments** across departments and Crown corporations, identifying every workload — including SaaS riding on hyperscaler infrastructure — whose infrastructure parent is US-jurisdictioned.

STAGE 2 · 6–18 MONTHS

Protect the crown jewels

1. Mandate genuinely sovereign infrastructure for **classified and Protected B defence and intelligence workloads**; begin migrating Defence 365 and equivalents to Canadian-controlled systems with Canadian key custody, anchored on the SSC/NRC secure-compute facility.

2. **Strengthen the Investment Canada Act for AI and data assets**: mandatory pre-closing national-security review for foreign acquisitions of Canadian AI firms, data-centre operators, and large sensitive-data holders; distressed-asset acquisitions presumptively reviewable; CSE/CSIS consultation required.

STAGE 3 · 18 MONTHS–5 YEARS

Build the alternative

1. In future Sovereign Compute Infrastructure Program awards, **prioritize Canadian-owned-and-operated facilities** with Canadian key custody — no repeat of the CoreWeave operator pattern.

   BENCHMARK → At least one ≥100 MW Canadian-owned-and-operated AI facility online by 2028.

2. **Keep the champions Canadian-owned.** Deploy the $500-million Canadian Tech Growth Fund and federal equity stakes to anchor Cohere and its successors with patient capital before they enter the pre-scale acquisition window that claimed Element AI and North.

3. Adopt a calibrated **buy-Canadian / buy-allied-sovereign procurement preference** for sensitive workloads, and use the twelve international AI partnerships to assemble a non-US sovereign-stack option — studying SecNumCloud's ownership rules and their trade-law exposure before importing them.

CAVEATS

The strongest cases against this briefing, stated fairly

"Sovereign cloud is more expensive and less capable."

Largely true at the margin. Canadian and European sovereign providers lag hyperscalers on managed AI services, serverless, and ecosystem depth; AWS lists roughly 143 compliance certifications to OVHcloud's roughly 13. The defensible answer is tiering — sovereign infrastructure for classified and sensitive workloads, hyperscalers for the rest — not wholesale migration. This briefing recommends exactly that.

"Five Eyes integration is a feature, not a bug."

Canada benefits enormously from allied intelligence sharing, and that integration is a national asset. But there is a categorical difference between willing, policy-controlled sharing and structural, involuntary exposure. The first, Canada governs. The second, it does not — and the Merkel precedent shows allies exploit structural access when interests diverge.

"Canada free-rides on US security and can't afford autonomy."

A real tension. Full digital autarky is neither achievable nor desirable for a middle power. But infrastructure dependence is itself a vulnerability that a transactional administration has already shown willingness to convert into coercion — tariffs, the Diffusion Rule, Starlink-style leverage. The goal is resilience and optionality. In Minister Solomon's words: sovereignty does not mean solitude.

Methodological notes — what this briefing cannot certify.

(1) The "over 80%" figure is IDC Canada market research (2024), mis-attributed in some secondary sources as a government statistic; it is cited here as private market data. (2) The Defence 365 exposure is an analytical argument (Balsillie Papers, March 2026), not a documented disclosure event. (3) Maven and Operation Epic Fury figures derive from Pentagon and contractor public statements and journalism, and should be read as capability-class indicators, not independently audited operational data. (4) Microsoft's sovereignty pledges are corporate commitments that, by Microsoft's own sworn testimony, cannot override the CLOUD Act. (5) Several 2026-dated items — "AI for All," the December 2025 Microsoft deal, Epic Fury — are recent and may be revised as fuller documentation emerges. NPSI publishes its uncertainty alongside its findings.

SOURCES

Selected sources

[01] Treasury Board of Canada Secretariat, *White Paper: Data Sovereignty and Public Cloud*, issued June 25, 2018 (maintained through 2023).

[02] Balsillie Papers, "U.S. Cloud Act" (Canadian Data series), incl. Appleton analysis, March 11, 2026; citing IDC Canada, *Canadian Cloud Services Market Analysis*, 2024.

[03] French Senate, hearing testimony of Anton Carniaux, Microsoft France, June 10, 2025.

[04] US Code: CLOUD Act, 18 U.S.C. §2713 (2018); FISA Section 702 reauthorization (2024).

[05] Shared Services Canada, Evaluation of Cloud Services, 2024–25; Office of the Privacy Commissioner of Canada, Annual Report 2023–24.

[06] DND/CAF, *Artificial Intelligence Strategy*, March 7, 2024; CSE, *AI Strategy* and *Cyber Threats to Canada's Democratic Process: 2025 Update*.

[07] ISED, *Canadian Sovereign AI Compute Strategy* (Dec 2024); National Security Review of Investments — updated Guidelines (March 5, 2025); Sensitive Technology List (Feb 6, 2025).

[08] Prime Minister's Office, "AI for All" strategy announcement, June 4, 2026; The Register, "Canada wants its own AI, less reliance on US tech," June 4, 2026.

[09] Microsoft On the Issues, "Microsoft Deepens Its Commitment to Canada with Landmark $19B AI Investment," Dec 9, 2025; Brock University expert commentary (Haggart), Dec 16, 2025.

[10] Breaking Defense, "'Insatiable appetite' for AI: Maven usage surged for strikes on Iran," May 12, 2026; CSIS, "What Is Maven Smart System?"; C4ISRNET, May 30, 2024.

[11] Danmarks Radio et al., Operation Dunhammer disclosures, May 2021.

[12] Duke University Sanford School (Sherman et al.), *Data Brokers and the Sale of Data on U.S. Military Personnel*, Nov 6, 2023.

[13] Fengate Asset Management / eStruxture recapitalization announcements, June–October 2024.

[14] PMO remarks on Telesat Lightspeed, March 9, 2026; Telesat/MDA contract, December 2024.

[15] US Department of Commerce, BIS: AI Diffusion Rule (Jan 15, 2025) and rescission (May 13, 2025); ITIF, "France's Cloud Service Restrictions," May 25, 2025.

ABOUT NPSI

The North Pacific Strategy Initiative publishes original, open-source geopolitical research on sovereignty, energy, technology, and the Pacific order. All sources unclassified. All uncertainty disclosed.

CITATION

James, Jesse. *Zero Secrets: Canada's Data and AI Sovereignty Crisis.* NPSI Special Briefing SB-01. North Pacific Strategy Initiative, June 11, 2026. npsi.ca

CONTACT

npsi.ca · linkedin.com/in/jessecares · Companion to NPSI WP05, *Sovereign Compute North* (forthcoming).